

REMARKS

In the above-noted Official Action, the Examiner objected to the specification at page 5 for an informality. Claim 1-7 were rejected under 35 U.S.C. §103(a) over MICALI (U.S. Patent No. 5,666,420) in view of ANGEBAUD et al. (U.S. Patent No. 5,218,637). In view of the herein-contained amendments and remarks, Applicants respectfully request reconsideration and withdrawal of each of the outstanding objections and rejection.

Initially, Applicants note that the specification has been amended at page 5, lines 1-6. In this regard, as the Examiner's interpretation of the specification at page 5 is correct, Applicants have adopted the Examiner's suggestion with respect to the interpretation of the specification at page 5, and have amended the same accordingly.

Applicants traverse the rejection of claims 1-7 under 35 U.S.C. §103(a) over MICALI in view of ANGEBAUD. In this regard, claims 1-7 have been cancelled without prejudice to or disclaimer of the subject matter recited therein. Claims 8-18 have been added for consideration by the Examiner. Claims 8-18 generally correspond to claims 1-7 with revisions to ensure that features recited in claims 8-18 are not interpreted as unduly limiting means-plus-function or steps-of limitations. Additionally, claims 8-18 have been amended to more clearly recite the distinctions between the various features recited in the claims. For example, claim 8 now separately recites, e.g., first digital data, encrypted first

P19949.A05

digital data, unencrypted first digital data and decrypted first digital data, so as to more clearly recite the features of the method. Additionally, multiple dependencies have been eliminated and additional claims added to specify singular dependency for each dependent claim now pending.

The outstanding Official Action asserts that the features recited in claim 1 are disclosed by MICALI, except that "the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party is valid". However, the outstanding Official Action asserts that, in view of ANGEBAUD, "it would have been obvious... to implement the claimed invention by... sending the unencrypted first digital data after establishing the trust there by to eliminate the need to decrypt the first digital data... the second party has no need to decrypt the first digital data thereby saving time in decrypt algorithm computation". Applicants respectfully assert that the above-noted Official Action is in error for at least each and all of the reasons set forth below.

MICALI is directed to an electronic transaction protocol which allows two parties to perform simultaneous transactions with minimum help from a trusted third party. The protocol requires that a first party (A) compute an encryption (z) in the third party's (Post Office's) public key of a triplet, i.e., $E_{PO}((A, B, E_B(m)))$. The triplet consists of identifiers (A) for the first party, (B) for the second party, and $(E_B(m))$ for the message (m)

encrypted in the second party's (B's) key. The message (m) from A to B is generally analogous to the first digital data of the present invention, and the encryption in the Post Office's public key of the message, i.e. (z), is generally analogous to the encrypted first digital data of the present invention. The first party (A) sends the encrypted message (z) to the second party (B). The second party (B) signs the received encrypted message (z) and sends it to the first party (A) as a receipt. If the first party (A) receives the properly signed receipt from the second party (B), the first party sends the second party the key to decrypt the encrypted message (z) and thereby obtain the message (m).

In other words, the first party (A) does not provide the second party (B) with any means to verify whether the encrypted message (z) is an encryption of the message (m), i.e., if the underlying message (m) is authentic. Moreover, MICALI emphasizes at column 6, lines 34-39 that the second party (B) must be unable to verify the encrypted data for the protocol to work, such that the second party is forced to provide the receipt to obtain the key to obtain the message (m).

Accordingly, the second party in MICALI is providing the receipt "blindly", i.e., without any verification of the authenticity of the encrypted first data. In contrast, the present invention recited in claim 8 provides assurances to the second party in the form of an authentication certificate, such that a receipt is provided by the second party contingent upon the second party being assured, e.g., by receiving the authentication certificate that

P19949.A05

the encrypted first digital data is an encryption of the first digital data. Therefore, MICALI does not provide any teaching of an "authentication certificate" as in the present invention, let alone an "authentication certificate authenticating that the encrypted first digital data is an encryption of the first digital data", as is recited in claim 8. Furthermore, MICALI does not disclose any feature similar to "the first party... sending the encrypted first digital data and the authentication certificate to the second party", as is recited in claim 8. Moreover, MICALI does not disclose any feature similar to "the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate", as is recited in claim 8. Additionally, MICALI does not disclose any feature similar to "the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data", as is recited in claim 8.

Accordingly, the present invention allows the second party to verify the authenticity of the encrypted data before sending a receipt in the form of the second digital data. This ensures fairness for the second party which cannot be provided by MICALI.

Additionally, as was noted above, the outstanding Official Action admits that MICALI does not disclose "the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party is valid".

However, the outstanding Official Action asserts that the above-noted feature is disclosed in ANGEBAUD et al. at column 9, lines 29-51. Applicants submit that the above-noted assertion is in error.

In particular, ANGEBAUD is directed to a method of transferring a secret by the exchange of two certificates between a card microcomputer and a security module microcomputer. The card microcomputer (first party) transmits towards the security module's microcomputer (second party) a first certificate comprising the credentials of the card as well as the signature of exponential X and optional message M (i.e., the first digital data of the present invention). However, at a later computational stage, after the security module microcomputer (second party) sends the second certificate (i.e., second digital data) to the card microcomputer (first party), the card microcomputer verifies the second certificate, and if valid, the card microcomputer calculates the exponential Y which provides the common transitory secret key to extract the secret. However, there is no disclosure of the card microcomputer sending unencrypted message M to the security module microcomputer. Moreover, not only does ANGEBAUD not disclose the above-noted feature recited in claim 8, but there is also no reason in ANGEBAUD to provide such a feature. In particular, there is no reason for the card microcomputer to send the unencrypted message M to the security module microcomputer, as the card

P19949.A05

microcomputer has already obtained the secret key/secret, such that sending the unencrypted message M would not provide a benefit.

Accordingly, contrary to the assertion of the above-noted Official Action, ANGEBAUD does not disclose or suggest "the first party verifying that the second digital data is valid and, when the second digital data is valid, the first party accepting the second digital data and sending the unencrypted first digital data to the second party", as is recited in claim 8. Moreover, as is noted above, the outstanding Official Action admits that the above-noted feature is not disclosed or suggested by MICALI.

Accordingly, at least for each and all of the reasons noted above, Applicants respectfully submit that claim 8 is allowable over the references applied in the outstanding Official Action. Applicants additionally submit that each of claims 9-18 are allowable, at least for depending from an allowable independent claim 8, as well as for additional reasons related to their own recitations. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the outstanding rejections and objections, as well as an indication of the allowability of each of the claims now pending.

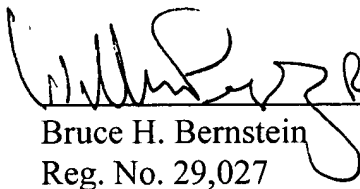
SUMMARY AND CONCLUSION

Applicants have made a sincere effort to place the present application in condition for allowance, and believe that they have now done so. Applicants have submitted new claims and shown how the combination of features recited in Applicants' claims are not taught, disclosed nor rendered obvious by the references cited by the Examiner.

Any amendments which have been made in this amendment, and which have not been specifically noted to overcome a rejection based upon the prior art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

Should the Examiner have any questions, the Examiner is invited to contact the undersigned at the below-listed telephone number.

Respectfully submitted,
Feng BAO et al.

 Reg. No. 29,027
Bruce H. Bernstein
Reg. No. 29,027

April 30, 2004
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191